UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

CITY OF ALMATY, KAZAKHSTAN, and BTA BANK JSC,

Plaintiffs,

-against-

MUKHTAR ABLYAZOV, VIKTOR KHRAPUNOV, ILYAS KHRAPUNOV, and TRIADOU SPV S.A.,

Defendants.

ORDER

1:15-CV-05345 (AJN) (KHP)

KATHARINE H. PARKER, UNITED STATES MAGISTRATE JUDGE

On August 2, 2017, Defendants Viktor and Ilyas Khrapunov (the "Khrapunovs") moved for reconsideration (doc. no. 389) of this Court's Order dated July 19, 2017 (doc. no. 369) granting in part and denying in part the City of Almaty, Kazakhstan's and BTA Bank JSC's (the "Kazakh Entities" or "Plaintiffs") motion for a protective order barring the use of stolen documents in this litigation (doc. no. 356). For the reasons set forth below, the motion is DENIED.

BACKGROUND

As discussed in more detail in this Court's July 19, 2017 Order, during a deposition of BTA Bank's corporate representative, Nurlan Nurgabylov, the Khrapunovs sought to use certain documents that they represented were documents stolen from the government of Kazakhstan via computer hacking and posted on a publicly available website called Kazaword. The Kazakh Entities stated that Nurgabylov could not authenticate the documents, which had only been produced to the Kazakh Entities on the eve of the deposition. The Kazakh Entities did not concede that the documents were obtained from the Kazaword website. They further

represented to this Court that they do not have a complete set of documents posted on Kazaword, that the hacked documents are no longer available on Kazaword, and that they have no way to determine whether the documents produced to them and referred to during Nurgabylov's deposition are actually copies of hacked documents posted to the Kazaword website. For this reason, the Kazakh Entities stated that they did not allow Nurgabylov to authenticate the documents. Put simply, the Kazakh Entities do not know whether the documents produced by the Khrapunovs are authentic copies of documents belonging to Kazakhstan that were in fact hacked and posted to the Kazaword website.

The Khrapunovs filed a motion to continue the deposition of Nurgabylov because of Plaintiffs' counsel's refusal to permit Nurgabylov to authenticate the documents. In response, Plaintiffs sought a protective order prohibiting use of the documents altogether in this action.

Separate from the instant action, a lawsuit alleging that Ilyas Khrapunov was involved in hacking the Kazakhstan government's documents and facilitating their posting on the Kazaword website is pending in the Northern District of California. *See Republic of Kazakhstan v. Ketebaev and Khrapunov*, No. 5:17-cv-00246 (LHK) (N.D. Cal. Jan. 20, 2017). Further, an injunction issued by the Honorable Edgardo Ramos enjoins those responsible for the hacking from using, disseminating, and publishing the hacked documents. *See Republic of Kazakhstan v. Does 1-100*, No. 15-cv-1900 (ER), 2015 WL 6473016 (S.D.N.Y. Oct. 27, 2015)

Because it is unclear whether the documents in question were among the hacked documents posted to the Kazaword website and whether Ilyas Khrapunov is responsible for the hacking, the motion for a protective order was premature insofar as it sought to preclude use of the documents in their entirety in this litigation. However, this Court concluded that the Kazakh

Entities' motion was not premature insofar as it sought a protective order limiting use of the documents in depositions given the allegations of Khrapunov's involvement in the hacking. In light of the parties' inability to compromise on even minor discovery disputes and in order to minimize future disputes by guiding the parties regarding upcoming depositions, this Court limited the use of the allegedly stolen documents in this matter. This Court held that the Khrapunovs may only (i) ask questions in depositions informed by the hacked documents and (ii) use the documents to refresh a witness's recollection, so long as the documents are not ones that constitute communications between Kazakhstan and its outside counsel or are otherwise plainly subject to a privilege. This Court also stated that at this juncture, the documents may not be introduced as deposition exhibits and Plaintiffs' witnesses shall not be required to authenticate a hacked document during a deposition while the California case is pending.

This Court also held that to the extent certain hacked documents are needed in this action as trial exhibits or exhibits to a dispositive motion and the California suit has not been resolved, the Khrapunovs shall write to this Court or Judge Nathan, as appropriate, to seek further direction. It further stated that to the extent the California action is resolved in their favor, the Khrapunovs may move for relief from this Court's Order; and, alternatively, to the extent the California action is resolved in the Plaintiffs' favor and Ilyas Khrapunov is deemed to have been involved in the hacking of the documents, the Injunction issued by Judge Ramos shall govern.

Through its Order, this Court sought to avoid having the Kazakh Entities repeatedly directing witnesses not to authenticate documents and creating transcripts with multiple

objections and potentially confusing testimony while still permitting the Khrapunovs to ask questions concerning information contained within the documents. Nevertheless, the Khrapunovs seek reconsideration of this Court's ruling insofar as it precludes them from introducing the hacked documents as deposition exhibits.

DISCUSSION

Motions for reconsideration are governed by Federal Rules of Civil Procedure 59(e) and Local Rule 6.3. "A motion for reconsideration should be granted only when the defendant identifies an intervening change of controlling law, the availability of new evidence, or the need to correct a clear error or prevent manifest injustice." *Kolel Beth Yechiel Mechil of Tartikov, Inc. v. YLL Irrevocable Trust*, 729 F.3d 99, 104 (2d Cir. 2013) (internal quotation marks omitted). The standard "is strict, and reconsideration will generally be denied unless the moving party can point to controlling decisions or data that the court overlooked." *Analytical Surveys, Inc. v. Tonga Partners, L.P.*, 684 F.3d 36, 52 (2d Cir. 2012) (internal quotation marks omitted). The decision to grant or deny a motion for reconsideration under Local Rule 6.3 and Rule 59(e) rests within "the sound discretion of the district court." *See Aczel v. Labonia*, 584 F.3d 52, 61 (2d Cir. 2009).

The Khrapunovs argue that this Court's ruling is "contrary to controlling precedent and is effectively a sanction." They argue that the Court has no authority to issue a sanction under Federal Rule of Civil Procedure 26(c) ("Rule 26"), and the Court cannot exercise its inherent equitable power to sanction the Khrapunovs without evidence of wrongdoing by the Khrapunovs and a finding of bad faith, neither of which are present here. They explain that because the allegations that Ilyas Khrapunov was responsible for the hacking are simply

allegations at this point, and because the documents were obtained from the Kazaword website, this Court lacks authority to sanction the Khrapunovs by limiting use of the hacked documents in depositions. Based on the above, they contend that this Court misapplied the holdings of *Fayemi v. Hambrecht & Quist, Inc.*, 174 F.R.D. 319, 323-24 (S.D.N.Y. 1997) and *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 568 (S.D.N.Y. 2008). They also cite to *Bridge C.A.T. Scan Assocs. v. Technicare Corp.*, 710 F.2d 940, 947 (2d Cir. 1983), a case not previously cited by the Khrapunovs to this Court.

In *Bridge C.A.T. Scan Associates,* the Second Circuit heard an appeal from a protective order issued by the district court pursuant to Rule 26(c) prohibiting disclosure of certain purportedly proprietary information attached as an exhibit to the plaintiff's complaint.[1] 710 F.2d 940. The information was a list of defendant's customers, their purchases, prices for equipment purchased, and installation dates of equipment. *Id.* at 942. Defendant asserted that the information had been obtained by plaintiff by improper means. *Id.* The court found that the nondisclosure order was a prior restraint on free speech and thus infringed on the plaintiff's First Amendment rights. *Id*. at 946-47. It also found that the order was contrary to historic principles of equity absent evidence of possible misconduct relating to misappropriation of the proprietary information. *Id*. at 946. The court recognized that Rule 26 grants the court power to impose conditions on *discovery*, but stated that the Rule is not a blanket authorization to prohibit *disclosure* of information. *Id*. at 944.

[1] The Second Circuit treated the appeal as a petition for writ of mandamus vacating the nondisclosure order because the non-final order was not appealable.

Fayemi involved a ruling on a defendant employer's motion to dismiss the complaint or, alternatively, preclude the plaintiff-employee's use of bonus information pertaining to other employees that he wrongfully removed from his supervisor's private office. 174 F.R.D. 319. After an evidentiary hearing, the court found that the plaintiff wrongfully obtained the bonus information but that the defendant also engaged in misconduct by failing to preserve the bonus information after commencement of the litigation. *Id*. at 322-23. The court held that Rule 26(c) did not authorize the court to preclude use of evidence obtained prior to commencement of litigation and independently of judicial process but found that courts have the inherent equitable power to prevent abuses, oppression, and injustices. *Id.* at 323-325. Nevertheless, because of defendant's unclean hands and the relevance of the information, the court declined to sanction the plaintiff. *Id.* at 326-27. Importantly, and pertinent to the instant motion, the court recognized that an order under Rule 26(c) may be granted "[u]pon motion by a party or by the person from whom discovery is sought," and the Rule therefore grants District Courts the power to "limit or foreclose discovery or regulate the disclosure of information obtained in discovery." *Id*. at 323.

Finally, in *Pure Power Boot Camp*, the court considered whether certain emails obtained by the plaintiff by secretly accessing a former employee's private email in violation of the federal Stored Communications Action, 18 U.S.C. § 2707, could be used in the litigation. 587 F. Supp. 2d 548. The plaintiff found the employee's password on the company's computer and then used it to access the employee's private email accounts. *Id*. at 552. The court noted that sanctions pursuant to the Federal Rules of Civil Procedure were not applicable because the misconduct occurred prior to the filing of the litigation and outside the normal discovery

process. *Id.* at 568. It nevertheless found that it had inherent equitable power to sanction a party that seeks to use evidence wrongfully obtained. *Id*. Accordingly, the court held that the emails should be precluded from use in the litigation except for impeachment purposes should defendants open the door. *Id.* at 571.

This Court noted the standard for issuance of a protective order in connection with stolen documents by citation to *Fayemi* and *Pure Power Boot Camp* but held that a protective order under this standard was premature because the California District Court has not yet determined if Ilyas Khrapunov was responsible for the hacking. However, in light of the necessity to address the dispute over the use of the documents during depositions in the meantime, the Court fashioned a ruling based on its power to control discovery under Rule 26. Thus, this Court did not misapply *Fayemi* or *Pure Power Boot Camp*. Nor was its Order contrary to *Bridge C.A.T. Scan Associates.*

Rule 26(c) provides that, "[a] party or any person from whom discovery is sought may move for a protective order in the court where the action is pending." Fed. R. Civ. P. 26(c). It further provides that "[t]he court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including one or more of the following: . . . specifying terms, including time and place . . . for . . . discovery. . . [and] forbidding inquiry into certain matters, or limiting the scope of disclosure or discovery to certain matters." *Id*. This is precisely what this Court did, although it did not repeat a citation to Rule 26 when making its ruling.

Unlike the sanctions cases discussed above, this Court did not prohibit the Khrapunovs from disclosing the hacked documents. It did not preclude use of the hacked documents as

evidence at trial or in connection with dispositive motions. It did not require the return or destruction of the hacked documents. It did not forbid the Khrapunovs from using the hacked documents. Rather, its prior Order merely provided directions as to how the documents could be used in depositions to avoid future disputes regarding authentication of the documents and directions to witnesses regarding testimony about the documents. This is precisely the type of order authorized by Rule 26(c). Thus, no finding of misconduct in connection with the acquisition of the hacked documents was needed, and the sanctions cases cited above are inapplicable.[2] Rather, the Court evaluated whether there was good cause for prescribing how the documents could be used at depositions pending the outcome of the California action that accuses Ilyas Khrapunov of hacking the documents. Fed. R. Civ. P. 26(c)(1).

It is well established that Rule 26 "confers broad discretion on the trial court to decide when a protective order is appropriate and what degree of protection is required." *U.S. Commodity Futures Trading Comm'n v. Parnon Energy Inc.*, 593 F. App'x 32, 36 (2d Cir. 2014) (quoting *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 36 (1984)). A limitation on how a party uses a specific subset of documents during depositions falls comfortably within this broad power, and does not turn on a finding of bad faith or entail sanctions upon any party. *See also* Fed. R. Civ. P. 1 (court must construe rules to secure just, speedy, and inexpensive

[2] The Court notes, however, that there is some evidence of misconduct. The Khrapunovs have offered scant proof that the hacked documents were ever hosted on the Kazaword website or otherwise publicly-available. Ilyas Khrapunov has been named in a lawsuit over his involvement in the theft, and Plaintiffs' witness, Mr. Nurgabylov, identified two witnesses who he claims can testify to Ilyas Khrapunov's admissions and involvement in acts of computer hacking. *See Republic of Kazakhstan v. Ketebaev and Khrapuno*, No. 17-cv-00246 (LHK) (N.D. Cal, Jan. 20, 2017). Nevertheless, because the District Court in California will adjudicate Ilyas Khrapunov's involvement in the hacking, this Court declined to make a determination in this regard.

determination of every action); Fed. R. Civ. P. 30(d) (court may issue orders limiting scope and conduct of depositions). Thus, there is no basis to revisit and modify the Order.

Moreover, nowhere do the Khrapunovs define the so-called "Kazaword documents," and the Kazakh Entities have made clear that they have no independent ability to verify whether a particular hacked document was ever available on the Kazaword website. The Kazakh Entities rightly object to this Court explicitly allowing the Khrapunovs to confront their witnesses and require them to answer questions about an undefined universe of stolen materials which the Khrapunovs have not produced in full and which cannot be verified as among those that were stolen and in fact posted to the Kazaword website. The supposed need to "confront" deposition witnesses with documents will not be satisfied by confronting them with documents that cannot be confirmed as an authentic government document. Thus, there is little benefit to marking the documents as exhibits and confronting the witnesses with them in deposition, particularly when the Khrapunovs may show the documents to the witness to refresh recollection and may ask questions about information contained in the documents.

CONCLUSION

For the above mentioned reasons, the motion for reconsideration is DENIED. Further, to avoid on going disputes regarding the hacked documents, and in light of the Kazakh Entities' lack of clarity regarding the universe of hacked documents, the Khrapunovs shall provide the Bates Numbers of all documents produced by them that they contend were downloaded from the Kazaword website and constitute hacked documents.

SO ORDERED.

Dated: September 8, 2017
New York, New York

Katharine H Parker

KATHARINE H. PARKER
United States Magistrate Judge